상세보기

(54) **SYSTEM AND METHOD FOR GENERATING RANDOM NUMBERS**

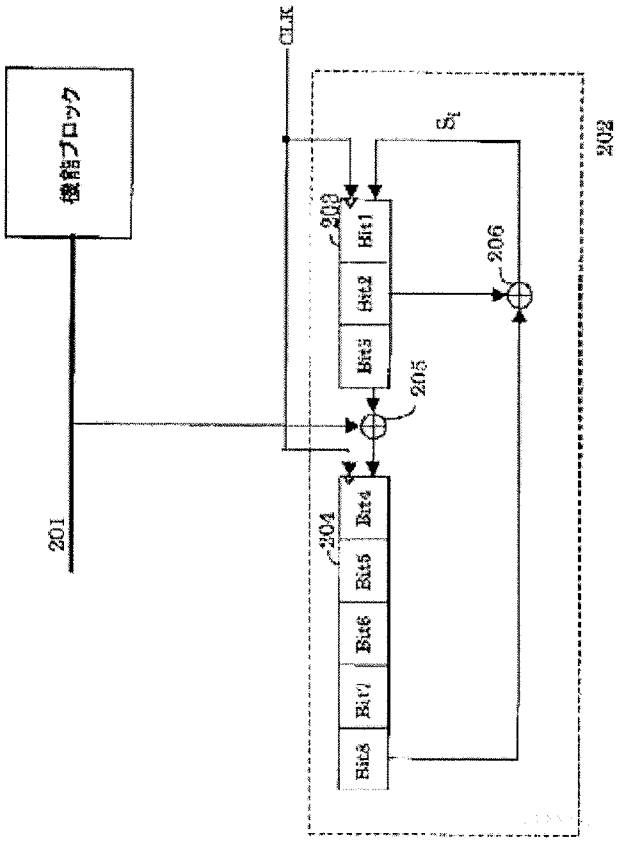
- (19) 국가 (Country) : JP (Japan)
- (11) 공개번호 (Publication Number) : **2003-122560** (2003.04.25) 日本語/한글(JP)
  현재진행상태보기
- (13) 문헌종류 (Kind of Document) : A (Unexamined Publication)
- (21) 출원번호 (Application Number) : 2001-319460 (2001.10.17)
- (75) 발명자 (Inventor) : MASANA YOSHIHIRO
- (73) 출원인 (Assignee) : OKI ELECTRIC IND CO LTD,

  대표출원인명 : OKI ELECTRIC INDUSTRY CO., LTD. (**A00535**)
- (57) 요약 (Abstract) :

PROBLEM TO BE SOLVED: To provide a system and a method for capable of generating highly irregular random numbers without cau consumption and an increase in chip size.

SOLUTION: This random number generating system comprises a ran for generating random numbers and a signal line 201 for transmitti installed on the outside of the random number generator 202. The ra comprises a first shift resister 203, a second shift resister 204, and logically operating an output from the first shift resister 203 and data line 201 and inputting the operated results to the second shift res data transmitted to a function block installed on the outside of the ra are utilized to generate the random numbers.

- 대표도면 :



- (51) 국제특허분류 (IPC) : G06F-007/58 ; G06K-019/07
- FI : G06F-007/58 A
  G06K-019/00 N
- 테마코드 : 5B035
- F텀 : **5B035:** AA00 BB09 BC00 CA11
- (30) 우선권번호 (Priority Number) : -
- 본 특허를 우선권으로 한 특허 : EP 1304613 A2 (2003.04.23)
  EP 1304613 A3 (2003.04.23)
  US 20030074380 A1 (2003.04.17)
- WIPS 패밀리 : WIPS 패밀리 보기

패밀리/법적상태 일괄보기

FullText Download

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（A）　(11)特許出願公開番号
特開2003－122560
（P2003－122560A）
(43)公開日　平成15年４月25日(2003.4.25)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ　５Ｂ０３５
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｎ

審査請求　未請求　請求項の数22　ＯＬ　（全 8 頁）

(21)出願番号　特願2001－319460(P2001－319460)

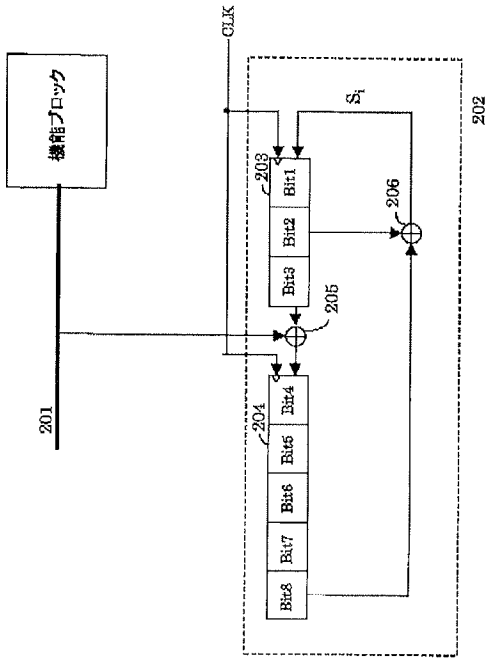
(22)出願日　平成13年10月17日(2001.10.17)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　正名　芳弘
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100089093
弁理士　大西　健治

Ｆターム(参考)　5B035 AA00 BB09 BC00 CA11

(54)【発明の名称】　乱数発生システム及び乱数発生方法

(57)【要約】
【目的】　消費電流の増大及びチップサイズの拡大を招くことなく、不規則性の高い乱数を発生する乱数発生システムおよび乱数発生方法を提供する。
【構成】　本発明に係る乱数発生システムは、乱数を発生する乱数発生器202と、乱数発生器202の外部に設けられた機能ブロックにデータを送信する信号線201とを有する。乱数発生器202は、第1のシフトレジスタ203と、第2のシフトレジスタ204と、第1のシフトレジスタ203の出力と信号線201により送信されるデータとを論理演算して、第2のシフトレジスタ204に入力する論理演算回路205とを有し、乱数発生器202の外部に設けられた機能ブロックに送信されるデータの値を利用して乱数を発生する。



【特許請求の範囲】
【請求項１】　乱数を発生する乱数発生器を有し、
前記乱数発生器は、前記乱数発生器の外部に設けられた機能ブロックに送信されるデータを利用して乱数を発生することを特徴とする乱数発生システム。
【請求項２】　前記乱数発生器は、第1のシフトレジスタと、
第2のシフトレジスタと、
前記第1のシフトレジスタから出力されたデータと、前記乱数発生器の外部に設けられた機能ブロックに送信されるデータとの論理演算を行い、演算結果を前記第2のシフトレジスタに出力する論理演算回路とを有することを特徴とする請求項1記載の乱数発生システム。
【請求項３】　ICカードに搭載されることを特徴とする請求項1若しくは2記載の乱数発生システム。
【請求項４】　前記乱数発生器の外部に設けられた機能ブロックに送信されるデータは、ICカードとICカードリードライタとの間で送受信されるデータであることを特徴とする請求項3に記載の乱数発生システム。
【請求項５】　前記乱数発生器の外部に設けられた機能ブロックに送信されるデータは、記憶装置に接続されたデータバスにより送信されるデータであることを特徴とする請求項1から3のいずれか一つに記載された乱数発生システム。
【請求項６】　前記機能ブロックは、中央演算処理装置であることを特徴とする請求項1から5のいずれか一つに記載された乱数発生システム。
【請求項７】　データ格納部を有する中央演算処理装置と、
前記データ格納部に格納されたデータに基づいて乱数を発生する乱数発生器とを有することを特徴とする乱数発生システム。
【請求項８】　前記乱数発生器は、第1のシフトレジスタと、
第2のシフトレジスタと、
前記第1のシフトレジスタから出力されたデータと、前記データ格納部に格納されたデータとの論理演算を行い、演算結果を前記第2のシフトレジスタに出力する論理演算回路とを有することを特徴とする請求項7記載の乱数発生システム。
【請求項９】　前記データ格納部は、アキュムレータであることを特徴とする請求項7若しくは8記載の乱数発生システム。
【請求項１０】　前記データ格納部は、汎用レジスタであることを特徴とする請求項7若しくは8記載の乱数発生システム。
【請求項１１】　前記データ格納部は、プログラムステータスワードであることを特徴とする請求項7若しくは8記載の乱数発生システム。
【請求項１２】　ICカードに搭載されることを特徴とする請求項7から11のいずれか一つに記載された乱数発生システム。
【請求項１３】　乱数発生器に初期値を設定するステップと、
前記乱数発生器の外部において使用されるデータに基づいて、前記乱数発生器において乱数を発生するステップとを有することを特徴とする乱数発生方法。
【請求項１４】　ICカードに搭載される乱数発生システムにおいて行われることを特徴とする請求項13記載の乱数発生方法。
【請求項１５】　前記データは、ICカードとICカードリードライターとの間で送受信されるデータであることを特徴とする請求項14記載の乱数発生方法。
【請求項１６】　前記データは、記憶装置に接続されたデータバスにより送信されるデータであることを特徴とする請求項13若しくは14記載の乱数発生方法。
【請求項１７】　前記データは、中央演算処理装置のデータ格納部に格納されたデータであることを特徴とする請求項13若しくは14記載の乱数発生方法。
【請求項１８】　前記データ格納部は、アキュムレータであることを特徴とする請求項17記載の乱数発生方法。
【請求項１９】　前記データ格納部は、汎用レジスタであることを特徴とする請求項17記載の乱数発生方法。
【請求項２０】　前記データは、プログラムステータスワードであることを特徴とする請求項17記載の乱数発生方法。
【請求項２１】　前記初期値は、予め発生しておいた乱数であることを特徴とする請求項13から20のいずれか一つに記載された乱数発生方法。
【請求項２２】　前記初期値は、中央演算処理装置のデータ格納部に格納されたデータであることを特徴とする請求項13から20のいずれか一つに記載された乱数発生方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は乱数発生システム及び乱数発生方法に関するものである。
【０００２】
【従来の技術】図５に従来の乱数発生システムを示す。従来の乱数発生システムとしては、線形フィードバックシフトレジスタ（以下、LFSRという。）を用いたものが知られている。LFSRを用いた従来の乱数発生器は、n段のシフトレジスタ（Si-1, Si-2, …, Si-n）501と、タップ列（C1, C2, …, Cn）502と、排他的論理和（XOR）回路群503とから構成される。
【０００３】シフトレジスタ501は、予め設定されている初期値データをクロック信号CLKに同期して1ビットずつ左へシフトさせる。タップ列502のC1, C2, …, Cnは、予め“０”又は“１”に設定される。n段のシフトレジスタ501のSi-1, Si-2, …, Si-nの値のうち、Ck=1 (1<k<n)

に設定されているものの排他的論理和が出力Siとなる。ここで、出力Siは

【外１】

$$(Si\text{-}1 \cdot C1) \oplus (Si\text{-}2 \cdot C2) \oplus \cdots \oplus (Si\text{-}n \cdot Cn)$$

の演算結果である。そして、このSiがシフト動作によりシフトレジスタ701のSi-1にフィードバック入力される。

【０００４】この従来の乱数発生器による乱数発生の手順は以下の通りに行われる。但し、手順（２）及び手順（３）は同時に行われる。

手順（１）：シフトレジスタ501に初期値を設定する。

手順（２）：各レジスタSi-1乃至Si-nは与えられた値を左にシフトする。

手順（３）予め“０”又は“１”に設定されたタップ列502に従って

【外２】

$$Si\text{-}1 \cdot C1 \oplus Si\text{-}2 \cdot C2 \oplus \cdots \oplus Si\text{-}n \cdot Cn$$

を計算し、最右端のレジスタSi-1にフィードバック入力する。ここで、演算子“・”は積を表し、

【外３】

“⊕”

は排他的論理和（XOR）を表す。

手順（４）：1ビットの乱数が必要な場合はSiを使用し、複数ビットの乱数が必要な場合はシフトレジスタ501の各レジスタから必要なビット分の値を出力して使用する。

【０００５】

【発明が解決しようとする課題】しかしながら、この従来の乱数発生器は、シフトレジスタ501の段数nと、予め設定されたタップ列502の値とにより、発生する乱数の周期が決定する。その結果、従来の乱数発生器では、同一の初期値が設定された場合、同一のタイミングに同一の乱数を発生し、このような構成では、不規則な乱数を得ることが難しかった。

【０００６】

【課題を解決するための手段】この発明に係る乱数発生システムは、前述の課題を解決するためになされたものであり、その代表的なものは、乱数を発生する乱数発生器を有し、この乱数発生器は、乱数発生器の外部に設けられた機能ブロックに送信されるデータを利用して乱数を発生することを特徴とする。

【０００７】

【発明の実施の形態】以下、本発明に係る乱数発生システムはICカードに搭載されるものとして説明する。

【０００８】〔第1の実施の形態〕本発明の第1の実施の形態に係る乱数発生システム及び乱数発生方法について説明する。まず、ICカードに搭載される半導体集積回路について図１を用いて説明する。図１は、ICカードに搭載される一般的な半導体集積回路を示すブロック図である。ICカードは、ICカードリードライタとデータ等の授受を行うコンタクト部101と、ICカードに搭載される半導体集積回路全体を制御する制御部102と、この制御部102が実行する制御プログラム等が格納される読み出し専用メモリ（以下、ROMという。）103と、制御部102が制御プログラムを実行する際に用いる書き込みと読み出しが可能なメモリ（以下、RAMという。）104と、取り引きデータ等主に可変するデータが格納される電気的に書き換え可能なROM（以下、EEPROMという。）105と、乱数を発生する乱数発生器106と、データバス107とから構成される。

【０００９】コンタクト部101は、ICカードリードライタの電源回路（図示せず。）から電源電圧及び接地電圧が供給される電源電圧端子VDD及び接地電圧端子GNDと、ICカードリードライタのクロック回路（図示せず。）からクロック信号が供給されるクロック端子CLKと、ICカードリードライタのリセット回路（図示せず。）からリセット信号が供給されるリセット端子RESと、ICカードリードライタのデータ入出力回路（図示せず。）からのシリアルデータが入力され、ICカードの制御部102からのデータをシリアルデータとしてICカードリードライタの入出力回路へ出力するデータ入出力端子SIOとから構成される。

【００１０】制御部102は、CPUであり、コンタクト部101から電源電圧、接地電圧、クロック信号、リセット信号、データが入力され、コンタクト部101のデータ入出力端子SIOへデータを出力する。

【００１１】乱数発生器106は、データバス107を介して制御部102及び記憶装置（ROM103、RAM104、EEPROM105）と接続される。この乱数発生器106において発生される乱数は、ICカードとICカードリードライタとの間で行われる暗証解読や、データバス107におけるスクランブル伝送に用いられる。

【００１２】ICカードとICカードリードライタとの間では、ICカードのデータ入出力端子（以下、SIO端子という。）とICカードリードライタのデータ入出力回路とを介してシリアルデータの授受が行われる。このデータは、取り引き情報等であり、乱数発生器の外部、例えばCPU等に送信され処理されるデータである。ICカードと外部機器であるICカードリードライタとの間で行われるデータの授受は、調歩同期で行われるため、シリアルデータは、非同期のタイミングで変化する。また、ICカードとリードライタとの間で授受されるデータ内容が異なると、当然、このシリアルデータパターンは変化する。本実施の形態は、このシリアルデータに基づいて、乱数を発生するものである。

【００１３】図2は、本発明の第1の実施の形態の構成を示す回路図である。本実施の形態に係る乱数発生システムは、信号線201と、信号線201のデータを利用して乱数を発生する乱数発生器202とから構成される。

【００１４】信号線201は、機能ブロックに接続される。機能ブロックとは、CPU若しくは記憶装置（ROM、RAM、EEPROM）等である。これらCPUや記憶装置は、本発明に係る乱数発生システムのために新たに設けられたものではなく、一般的にICカードに搭載されるものである。信号線201により送信されるデータは、ICカードとICカードリードライタとの間で送受信されるシリアルデータである。

【００１５】乱数発生器202は、線形フィードバックシフトレジスタ（LFSR）を用いたものである。この乱数発生器202は、クロック信号CLKに同期して予め設定されている初期値データを左に1ビットずつシフトさせる第1のシフトレジスタ203及び第2のシフトレジスタ204と、信号線201により送信されるデータ、すなわちICカードのSIO端子を介してICカードリードライタとの間で送受信されるシリアルデータと、第1のシフトレジスタ203の出力との論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する論理演算回路（XOR回路）205と、第1のシフトレジスタ203のレジスタBit2の出力と第2のシフトレジスタ204の出力との論理演算を行い、その演算結果Siを第1のシフトレジスタ203にフィードバック入力する論理演算回路（XOR回路）206とから構成される。

【００１６】本実施の形態では、第1のシフトレジスタ203を、レジスタBit1乃至レジスタBit3の3ビット構成とし、第2のシフトレジスタ204を、レジスタBit4乃至レジスタBit8の5ビット構成としているがこれに限られるものではない。また、本実施の形態では、第1のシフトレジスタ203のレジスタBit2の値と、第2のシフトレジスタ204のレジスタBit8の値との論理演算（排他的論理和）結果Siを第1のシフトレジスタ203にフィードバック入力しているが、これに限られるものではなく、レジスタBit1乃至レジスタBit8の任意かつ複数のレジスタからの出力を論理演算して、その演算結果を第1のシフトレジスタ203にフィードバック入力させてもよい。

【００１７】次に、本実施の形態に係る乱数発生システムにおける乱数発生方法について説明する。この本実施の形態に係る乱数発生システムにおける乱数発生の手順は以下の通りに行われる。但し、手順（２）～手順（４）は同時に行われる。

手順（１）：第1のシフトレジスタ203及び第2のシフトレジスタ204に初期値データを設定する。

手順（２）：各レジスタは、与えられた値をクロック信号CLKに同期して順次左へ1ビットずつシフトさせる。

手順（３）：論理演算回路（XOR回路）205は、第1のシフトレジスタ203の出力と、信号線201により送信されるデータ（SIO端子を介してICカードリードライタとの間で送受信されるシリアルデータ）との論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する。

手順（４）：論理演算回路（XOR回路）206は、第1のシフトレジスタ203のレジスタBit2の出力と、第2のシフトレジスタ204の出力との論理演算（排他的論理和）を行い、その演算結果Siを第1のシフトレジスタ203にフィードバック入力する。

手順（５）：1ビットの乱数が必要な場合はSiを使用し、複数ビットの乱数が必要な場合は第1のシフトレジスタ203及び第2のシフトレジスタ204の任意のレジスタから必要なビット分の値を出力して使用する。

【００１８】手順（１）において、第1のシフトレジスタ203及び第2のシフトレジスタ204に設定される初期値には、前回ICカードを使用した時に発生し記憶装置に格納しておいた乱数を用いる。

【００１９】また、手順（１）において、第1のシフトレジスタ203及び第2のシフトレジスタ204に初期値を設定する手段としては、乱数発生器202の周辺に設けられた中央演算処理装置のデータ格納部に格納されたデータを用いることも可能である。

【００２０】以上説明したように、本実施の形態に係る乱数発生システムは、乱数発生器の外部に設けられた機能ブロック（中央演算処理装置若しくは記憶装置）に送信され使用されるデータ、例えば、ICカードとICカードリードライタとの間で送受信されるシリアルデータと、第1のシフトレジスタ203の出力との論理演算を行い、その演算結果を第2のシフトレジスタ204に入力することにより、不規則性の高い乱数を発生することができ、かつ、乱数発生器202の外部に新たな回路を設けないため、消費電流の増大及びチップサイズの拡大を回避することができる。

【００２１】〔第2の実施の形態〕次に、本発明の第2の実施の形態係る乱数発生システムについて図3を参照して説明する。図3は、本発明の第2の実施の形態に係る乱数発生システムの構成を示す回路図である。本実施の形態に係る乱数発生システムにおいて、図２に示す第1の実施の形態に係る乱数発生システムと異なる点は、図２における信号線201が信号線（データバス）301に変更されている点である。その他の回路構成は、図3に示す第1の実施の形態に係る乱数発生システムと同一であるため同一の符号を付して説明する。

【００２２】データバス301は、本発明により新たに設けられたものではなく、従来からICカードに搭載される機能ブロック間に設けられているデータバスである。ここで、機能ブロックとは、CPUや記憶装置であるROM、RAM、EEPROM等である。

【００２３】これら機能ブロック間を接続するデータバス301により送信されるデータは、CPUがROM、RAM、EEPR

OMにアクセスする度に変化するものである。また、データバスにより送信されるデータは、クロック信号に同期して送信されるものであるが、各記憶装置（ROM、RAM、EEPROM等）のアクセスタイムがそれぞれ異なることにより、データバス上のデータパターンは不規則に変化する。その結果、データバス301から論理演算回路（XOR回路）205に入力されるデータの不規則性が高まり、論理演算回路（XOR回路）205から第2のシフトレジスタ204に入力されるデータの不規則性が高まることとなる。

【００２４】ICカードに搭載される乱数発生システムにおける記憶装置（ROM、RAM、EEPROM等）に書き込まれるデータ、又は、これら記憶装置から読み出されるデータは、各ICカードごとに異なり、さらには、ICカードが使用される度に変化するものである。その結果、データバス301から論理演算回路205に入力されるデータの不規則性が高まり、論理演算回路205から第2のシフトレジスタ204に入力されるデータ値の不規則性が高まることとなる。

【００２５】次に、本実施の形態に係る乱数発生システムにおける乱数発生方法について説明する。本実施の形態に係る乱数発生システムにおける乱数発生方法において、第1の実施の形態に係る乱数発生システムにおける乱数発生方法と異なる点は、手順（３）であるため、手順（３）についてのみ説明する。

手順（３）：論理演算回路（XOR回路）205は、第1のシフトレジスタ203の出力と、信号線（データバス）301により送信されるデータの値との論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する。

【００２６】以上説明したように、本実施の形態に係る乱数発生システムは、複数の機能ブロック（CPUや記憶装置等）間を接続するデータバスにより送信されるデータの値と、第1のシフトレジスタ203の出力との論理演算を行い、その演算結果を第2のシフトレジスタ204に入力することにより、不規則性の高い乱数を発生することができ、かつ、乱数発生器202の外部に新たな回路を設けないことにより、消費電流の増大及びチップサイズの拡大を回避することができる。

【００２７】〔第3の実施の形態〕次に、本発明の第3の実施の形態に係る乱数発生システムについて図4を参照して説明する。図4は、本発明の第3の実施の形態の係る乱数発生システムの構成を示す回路図である。本実施の形態に係る乱数発生システムにおいて、図２に示した第1の実施の形態に係る乱数発生システムと異なる点は、図２における信号線201から論理演算回路（XOR回路）205に入力されるデータが、CPU401のデータ格納部402に格納されたデータに変更されている点である。ここで、CPU401は、本発明において新たに設けられたものではなく一般的にICカードに搭載されるものである。その他の回路構成は、図2に示す第1の実施の形態に係る乱数発生システムと同様であるため同一の符号を付して説明する。

【００２８】データ格納部402は、CPU401におけるアキュムレータ、若しくは、アキュムレータを有しないCPUであれば高い頻度で演算に使用される汎用レジスタである。このアキュムレータ若しくは汎用レジスタは、本発明により新たに設けられたものではなく、従来からCPUに設けられているものである。

【００２９】アキュムレータ（若しくは汎用レジスタ）402から論理演算回路（XOR回路）205に入力されるデータは、CPU401においてプログラムが処理される度に変化するデータである。また、このデータは、プログラム処理の流れが異なる場合や、CPUが演算を行う際に用いられるデータ、すなわち、外部機器から入力されるデータや記憶装置から読み出されるデータが異なることにより変化するものである。

【００３０】ICカードに搭載される乱数発生システムにおいて、CPUを構成するアキュムレータ（若しくは汎用レジスタ）402に格納されるデータは、外部機器であるICカードリードライタから供給されるデータ、又は、ICカードに搭載された記憶装置から読み出されるデータにより変化するものである。その結果、アキュムレータ（若しくは汎用レジスタ）402から論理演算回路205に入力されるデータ値の不規則性が高まり、論理演算回路205から第2のシフトレジスタ204に入力されるデータ値の不規則性が高まることとなる。

【００３１】次に、本実施の形態に係る乱数発生システムにおける乱数発生方法について説明する。本実施の形態に係る乱数発生システムにおける乱数発生方法において、第1の実施の形態に係る乱数発生システムにおける乱数発生方法と異なる点は、手順（３）であるため、手順（３）についてのみ説明する。

手順（３）：論理演算回路205は、第1のシフトレジスタ203の出力と、CPU401のアキュムレータ（若しくは汎用レジスタ）402に格納されたデータとの論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する。

【００３２】以上説明したように、本実施の形態に係る乱数発生システムは、CPU401を構成するデータ格納部（アキュムレータ若しくは汎用レジスタ）402に格納されたデータと、第1のシフトレジスタ203の出力との論理演算を行い、その演算結果を第2のシフトレジスタ204に入力することにより、不規則性の高い乱数を発生することができ、かつ、乱数発生器202の外部に新たな回路を設けないことにより、消費電流の増大及びチップサイズの拡大を回避することができる。

【００３３】〔第4の実施の形態〕次に、本発明の第4の実施の形態に係る乱数発生システム及び乱数発生方法について説明する。

【００３４】本実施の形態に係る乱数発生システムにおいて、第3の実施の形態に係る乱数発生システムと異な

る点は、第3の実施の形態におけるアキュムレータ（若しくは汎用レジスタ）401が、PSW（プログラムステータスワード）に変更されている点である。このPSWは、本発明により新たに設けられたものではなく、従来からCPUに設けられているものである。その他の回路構成は、図４に示した第3の実施の形態に係る乱数発生システムと同様である。従って、本実施の形態は、図４を参照して説明する。

【００３５】PSW402は、CPUにおける制御回路内に設けられている。この制御回路は、PSW402及びCPU内に設けられた命令デコードユニット（図示せず。）のデコード結果に従って、CPU内に設けられたメモリユニット（図示せず。）及び演算ユニット（図示せず。）を制御する。PSW402に格納されるデータは、例えば、演算キャリーや0（ゼロ）フラグ等の制御フラグである。この制御フラグは、CPU401においてプログラムが処理され、演算処理が行われることにより、複雑かつ不規則に変化するものである。

【００３６】本実施の形態では、このPSW402に割り付けられてた制御フラグ、例えば、演算キャリーや0（ゼロ）フラグ等、若しくはこれら複数の値の論理演算結果を論理演算回路205に入力して使用する。論理演算回路205は、このPSW402に格納されているデータと第1のシフトレジスタ203の出力との論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する。このPSWに格納されるデータは、プログラム処理の流れが異なる場合や、CPUが演算処理に用いるデータ、すなわち、外部機器から入力されるデータや記憶装置から読み出されるデータが異なることにより変化するものである。

【００３７】ICカードに搭載される乱数発生システムにおけるCPUに設けられたPSW402に格納されるデータは、外部機器であるICカードリードライタから供給されるデータ、又は、ICカードに搭載された記憶装置から読み出されるデータにより変化するものである。その結果、PSW402から論理演算回路（XOR回路）205に入力されるデータ値の不規則性が高まり、論理演算回路205から第2のシフトレジスタ204に入力されるデータ値の不規則性が高まることとなる。

【００３８】次に、本実施の形態に係る乱数発生システムにおける乱数発生方法について説明する。本実施の形態に係る乱数発生システムにおける乱数発生方法において、第3の実施の形態に係る乱数発生システムにおける乱数発生方法と異なる点は、手順（３）であり、その他は第3の実施の形態と同様であるため、手順（３）についてのみ説明する。

手順（３）：論理演算回路205は、第1のシフトレジスタ203の出力と、CPU内に設けられたPSW（プログラムステータスワード）402に格納されたデータの値との論理演算（排他的論理和）を行い、その演算結果を第2のシフトレジスタ204に入力する。

【００３９】以上説明したように、本実施の形態に係る乱数発生システムは、CPUに設けられたデータ格納部（PSW；プログラムステータスワード）402に格納されたデータと、第1のシフトレジスタ203の出力との論理演算を行い、その演算結果を第2のシフトレジスタ204に入力することにより、不規則性の高い乱数を発生することができ、かつ、乱数発生器202の外部に新たな回路を設けないことにより、消費電流の増大及びチップサイズの拡大を回避することができる。

【００４０】

【発明の効果】以上詳細に説明したように、この発明の代表的なものによれば、乱数を発生する乱数発生器を有し、この乱数発生器は、乱数発生器の外部に設けられた機能ブロックに送信されるデータを利用して乱数を発生することにより、消費電流の増大及びチップサイズの拡大を招くことなく、不規則性の高い乱数を発生することができる。

【図面の簡単な説明】

【図１】ICカードに搭載される一般的な半導体集積回路を示すブロック図

【図２】本発明の第１の実施の形態に係る乱数発生システムの構成を示す回路図

【図３】本発明の第２の実施の形態に係る乱数発生システムの構成を示す回路図

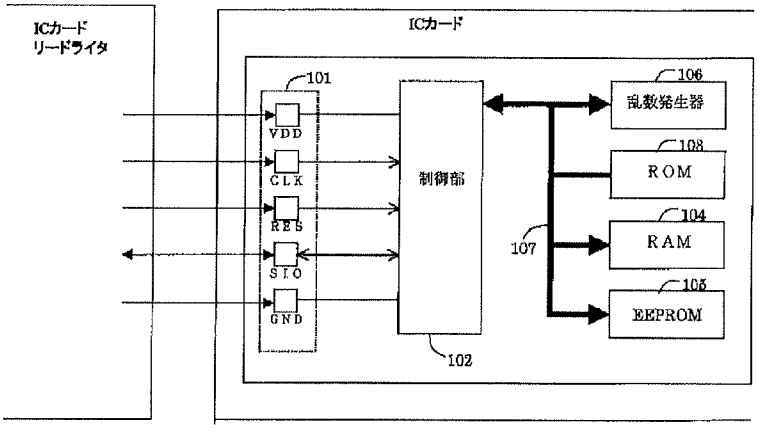
【図４】本発明の第３の実施の形態に係る乱数発生システムの構成を示す回路図

【図５】従来の乱数発生器を示す回路

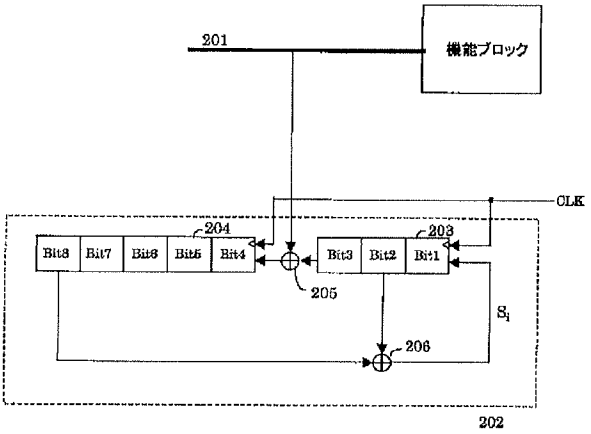
【符号の説明】

201　信号線
202　乱数発生器
203　第1のシフトレジスタ
204　第2のシフトレジスタ
205　206　論理演算回路

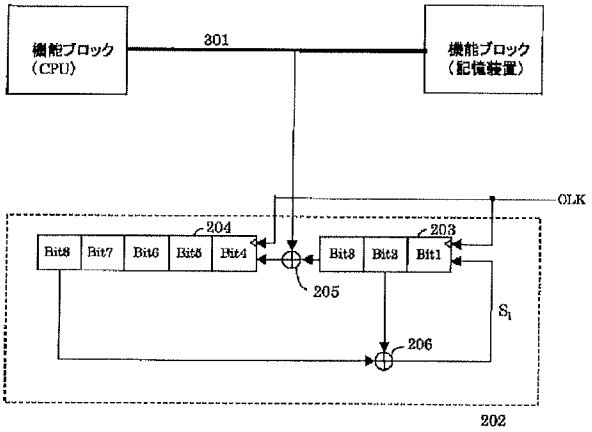
【図１】


ICカード
リードライタ
ICカード
101
VDD
CLK
RES
SIO
GND
制御部
102
106
乱数発生器
108
ROM
104
RAM
107
105
EEPROM

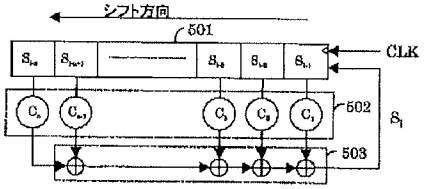
【図２】


201
機能ブロック
CLK
204
203
Bit8
Bit7
Bit6
Bit5
Bit4
Bit3
Bit2
Bit1
205
206
S_i
202

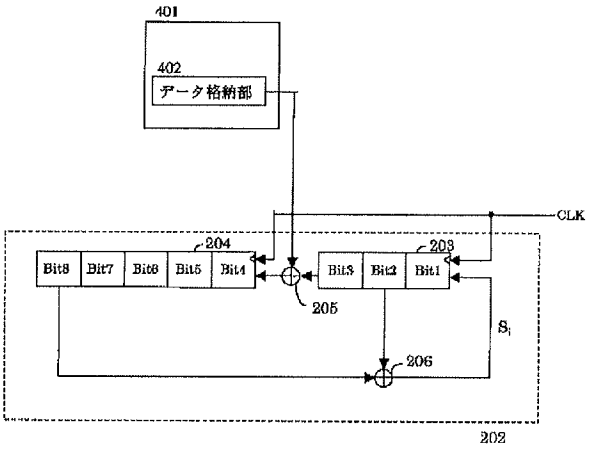
【図３】


機能ブロック
(CPU)
301
機能ブロック
(記憶装置)
CLK
204
203
Bit8
Bit7
Bit6
Bit5
Bit4
Bit3
Bit2
Bit1
205
206
S_i
202

【図５】


シフト方向
501
CLK
502
503
S_i

【図４】


401
402
データ格納部
CLK
204
203
Bit8
Bit7
Bit6
Bit5
Bit4
Bit3
Bit2
Bit1
205
S_i
206
202